

CSCI 124: Discrete Structures II: Discussion Session 4

Poorvi L. Vora

1. Find $\gcd(51, 30)$.
2. Consider the multiplicative cipher $f(x) = 5x \text{ MOD } 17$. What is its inverse? That is, what is the function $g(x)$ such that $g(f(x)) = x$?
3. You may assume that $x \in \mathbb{Z}_m$ has a multiplicative inverse modulo m if and only if $\gcd(x, m) = 1$. Show that $\mathbb{Z}_m \setminus \{0\}$ is a group with respect to multiplication modulo m if and only if m is prime.

In order to do problems 4a and 4b, first show the following, for integers x, y, z and positive integer m :

A.

$$((x \text{ rem } m) + (y \text{ rem } m)) \text{ rem } m = (x + y) \text{ rem } m$$

B.

$$((x \text{ rem } m) \times (y \text{ rem } m)) \text{ rem } m = (xy) \text{ rem } m$$

C.

$$[(z \text{ rem } m)((x \text{ rem } m) + (y \text{ rem } m))] \text{ rem } m = [z(x + y)] \text{ rem } m$$

(Hint: use the facts shown earlier: For integers a, b, c, d and positive integer m , if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $(a + c) \pmod{m} \equiv (b + d) \pmod{m}$ and $ac \pmod{m} \equiv bd \pmod{m}$.)

4a. (From quiz) Show that $H = \{x \in \mathbb{Z}_{26} \mid \text{such that } 13x = 0 \pmod{26}\}$ is a subgroup of $G = \mathbb{Z}_{26}$ with operation addition modulo 26.

4b. Show that $H = \{x \in \mathbb{Z}_5 \mid \text{such that } x^2 = 1 \pmod{5}\}$ is a subgroup of $G = \mathbb{Z}_5 \setminus \{0\}$ with operation multiplication modulo 5.

5. Consider group G with commutative operation \diamond and identity e . Given any $x \in G$, define $x^2 = x \diamond x$. Further, define $x^0 = e$ and x^k as $x^{k-1} \diamond x$. Show that $H = \{x \in G \mid \text{such that } x^n = e\}$ is a subgroup of G for all integers n such that $0 \leq n \leq |G|$ where $|G|$ is the size of G . Observe that 4a and 4b are special cases of this result.